draft-ietf-pppext-mppp-00

PPP-Extension Working Group
Internet-Draft
Expires June 1st, 1999

M. C. Chuah
Bell Labs
D. Grosser
IBM Corporation
G. Rai
Lucent Technologies
Jacob Teplitsky
RABU
Lucent Technologies

Mobile PPP (MPPP)
draft-ietf-pppext-mppp-00.txt

Status Of This Memo

Abstract

This document describes a new feature for L2TP: it allows for a change of LACs during the lifetime of a PPP session without the latency of re-creating a new PPP session where possible. This feature is specially useful for wireless data services where the foreign wireless service provider (WSP) may be different than the user's home service provider and where a user's mobility may result in a change of LAC during an on-going PPP session. This proposal presents 3 different methods of supporting this feature. The simplest method requires only minor changes to both LACs and LNSs. However, it may give a larger handover latency. The other two methods have shorter handover latency and allow us to extend the L2TP session by an additional hop.

Table of Contents

1.0 Introduction 2
1.1 Limitations of L2TP for wireless services.......................3
2.0 Overview of Mobile PPP..3
2.1 Simple AVP Approach 3
2.2 Independent Tunnel Approach.....................................4
2.3 Concatenated Tunnel Approach....................................6
3.0 Service Model Issues 7
3.1 Authentication 7
3.2 Accounting 7
4.0 Control Message Processing 8

4.1 Newly Defined Control Message and AVPs........................8
4.1.1 Authentication Request...8
4.1.2 Newly Defined AVPs...8

4.1.2.1 User AVP...9
4.1.2.2 Sequence Number AV 9
4.1.2.3 A-LAC's Window AVP 10
5.0 Security Issues 10
6.0 Acknowledgments 10
7.0 Contacts 10
8.0 References 11
Appendix 1: Using CTA in an Handover Scenario 11
Appendix 2: Transfer of Sequence Number During Handover 12
Appendix 3: Multiple LNS Scenario 12

1. Introduction

```
          Serving        PPP
           IWF          Server
           --             --          ---------
MN  <---> |  | <-------->|  | <----> R  ( Internet)
           --             --          ---------
MN: Mobile Node
R: Router
IWF: Interworking Function
```

Fig 1 Typical wide area wireless access network architecture

Fig 1 shows the architecture of a typical wide area wireless access network like CDMA, GSM, or TDMA. Current wireless standards allow mobile nodes (MN) to dial up a PPP server to access the internet. A link level tunnel is created between the serving IWF and the PPP server. If the mobile node moves to another serving IWF, link-layer messages are exchanged so that the tunnel between the old serving IWF and the PPP server is torn down and a new one set up between a new serving IWF and the PPP server. If the mobile node moves further such that it has to change the PPP server, then current wireless standards force a termination of the PPP session. A new PPP session has to be negotiated between the mobile node and the new PPP server. In addition, current wireless standards do not provide virtual private networking services to mobile nodes.

In current wireless architectures, the PPP server authenticates mobile nodes using the negotiated PPP authentication protocol e.g. CHAP. Since it is not aware of mobile node handovers in the wireless network, it does not perform any authentication when a mobile node changes its serving IWF.

In this document, we propose a mobile feature to the current IETF L2TP protocol to provide wide area mobility to nodes without having to renegotiate the PPP session during a handover. According to this proposal, mobile nodes need only implement the TCP/IP/PPP stack with no modifications. All current PCs and the future crop of hand held data devices are expected to have this stack.

There are three methods to provide this mobile feature, namely (a) Simple AVP Approach (SAA), (b) Independent Tunnel Approach (ITA), and (c) Concatenated Tunnel Approach (CTA). Both the SAA and ITA require changes to both LAC and LNS software but the CTA only requires changes to the LAC. We list the advantages and disadvantages of these 3 different approaches in later sections. We prefer CTA because it provides end-to-end flow control for the 2-hop PPP session and it requires less CPU processing compared to ITA.

This proposal is independent of the wireless access technologies. It provides hooks to carry mobile node security credentials between network access servers in a technology independent manner. It also makes no assumptions about the methods by which wireless terminals are identified or about the encryption and authentication methods used by the wireless networks.

1.1 Limitations of L2TP for wireless services

The current L2TP draft [1] does not allow for a transfer of Network Access Server (NAS) during an existing PPP session. In a cellular environment, a change of NAS may occur during the lifetime of a PPP session. A user may start a PPP session and move into another service provider's coverage area which has a different NAS.
The current L2TP draft forces the user to drop the currrent PPP session and renegotiate a new session. Instead of terminating the existing PPP session and starting a new one which takes time and can be expensive in high capacity, micro-cellular wireless networks, one solution is to let the old NAS (LAC) transfer the PPP session to the new NAS (LAC).

The current L2TP draft also does not allow mobile data users visiting a foreign wireless ISP to use the wireless ISP for virtual private networking services from an area where their home (wireless) ISP is not in operation.

2.0 Overview of Mobile PPP

There are three methods for providing the mobile feature. These methods differ in terms of their implementation complexity. The three methods are (i) Simple AVP Approach (SAA), (ii) Independent Tunnel Approach (ITA), and (iii) Concatenated Tunnel Approach (CTA).

2.1 Simple AVP Approach (SAA)

With the Simple AVP approach, both the existing LAC and LNS need to be enhanced to process the User AVP, a newly defined AVP.

```
--------             ----------
| Old   | Tunnel=2   |         |
|  LAC  |   ----------| LNS     |
--------  callid=5   ---------
                       /
                      /
                     / Tunnel=3, callid=1
```

```
                 ---------
                | New LAC |
                 ---------
```

```
       New LAC                   LNS       Old LAC
Link
Msg 1    SCCRQ
--->    ----------------------->
         SCCRP (with Mobile AVP)
         <--------------------
         SCCCN
         -------------------->
         ICRQ (with User AVP)
         ---------------------->
                                  CDN
                                ----------->
         ICRP (with ACCM AVP, Proxy Auth AVP)
         <--------------------
         ICCN
         -------------------->
```

Fig 2 Simple AVP Approach

In Fig 2, we assume that the link layer message contains some subscriber information. Such information allows the new LAC, via the help of its local AAA server, to determine which LNS the new LAC should talk to. We assume that when a tunnel is set up between a LAC and a LNS, the LNS will respond with a Mobile AVP in its SCCRP message if it does support the mobility feature. In addition, the LNS will interpret any ICRQ with an attached User AVP as a possible signal of an handover for an existing PPP call. Using the information provided in the User AVP, LNS can use its local AAA server and its connection table to determine the identity of the old LAC which the subscriber previously communicates with.

If the LNS cannot accept the call handover, the LNS will send a CDN message to the new LAC. If the LNS can accept the handover, the LNS will send a Call Disconnect Notify (CDN) message to the old LAC. Next, the LNS replies with an ICRP message to the new LAC as stated in [1]. To support the handover feature, the ACCM AVP, and possibly the Proxy Authentication AVP need to be included in the ICRP message. We assume that the sequence numbers will be re-initialized at the LNS after the handover.

Note that we assume that the LAC does not initiate the teardown of L2TP session (unless a relatively long inactivity timer times out). Thus, there is no issue of LNS receiving a CDN message from the old LAC due to the handover before receiving the ICRQ message from the new LAC.

The advantage of SAA is :
(a) it is very simple.

The disadvantages of SAA are:
(a) Both the LAC and LNS software need to be updated to recognise the newly defined User AVP message.
(b) The handover latency may be long since the LAC may be located

within the WSP intranet while the LNS is located within the ISP or corporate network far away.
(c) Roaming service may be limited to a smaller geographical area because the LACs within the WSP intranets and the LNSs within a corporate network do not trust one another unless there is a direct agreement between different WSPs and the corporate network.

However, there may be cases where this approach is not secure or feasible. For such cases, we may need to extend the PPP session to a 2-hop session. A new entity called the Anchor LAC is introduced for the 2-hop session.

2.2 Independent Tunnel Approach (ITA)

In the Independent Tunnel Approach, there are two L2TP data sessions per PPP call: one between the Serving LAC and the Anchor LAC; one between the Anchor LAC and LNS. To the Serving LAC, the Anchor LAC looks like the LNS. To the LNS, the Anchor LAC looks like the LAC. The flow control procedure for the two data sessions is independent of one another. The Anchor LAC needs to provide a mapping table to map the tunnel and call identities of one data session to those of the related data session that belong to the same PPP call. Thus, the Anchor LAC has to maintain 2N data sessions for N PPP calls in ITA.

```
----------             --------
| Anchor | Tunnel=1   | LNS    |
| LAC    |------------|        |
 ---------  callid=3   --------
    |
    |
    |  Tunnel=3, callid=1
 -------------
|Serving LAC |
 -------------
```

```
S-LAC: Serving LAC          A-LAC: Anchor LAC

Client     S-LAC            A-LAC          LNS
   Link Layer
      Msg1       SCCRQ
   --------->  ---------->
                 SCCRP (with Mobile AVP)
               <---------
                 SCCCN
               ------------>
                 ICRQ (with User AVP)
               ------------->
                 ICRP  (with ACCM AVP, Proxy Auth AVP)
              <-------------
                 ICCN          Auth_Req (Optional)
               ------------->  ------->
                  ACK
                <----------
  Link Layer
     Msg2
  <---------
```

One hop to 2-hop Handover Scenario
Fig 3 Independent Tunnel Approach

In Fig 3, we assume that the mobile subscriber first establishes a PPP call between the Anchor LAC and the LNS (tunnelid=1, callid=3). Then, the mobile subscriber roams to the coverage area of another new LAC (referred to as the Serving LAC). From the link-layer handoff message, the Serving LAC discovers that there is an existing PPP call. Thus, the Serving LAC sends an ICRQ message which contains a User AVP. The Anchor LAC will first determine if this existing PPP call requests for an extended hop or for a change of LAC. Such a decision can be made with the help of the local AAA server and the information contained in the User AVP. Next, the Anchor LAC decides if this PPP call already has a 2-hop L2TP tunnel. If the Anchor LAC determines that this existing PPP call needs an extended hop, it will create an entry in its mapping table (MT) so that the L2TP headers of all packets with (tunnelid=1,callid=3) from the incoming interface can be swapped with an L2TP header with (tunnelid=3, callid=1) at the outgoing interface. If a user-level re-authentication is desired, the Anchor LAC can send an Authentication Request message (an optional newly defined L2TP control message) to the LNS.

```
--------               ----------          --------
|Serving| Tunnel=3     | Anchor | Tunnel=1  | LNS  |
|  LAC1 |   -----------| LAC    |-----------|      |
--------  callid=1     ---------  callid=3  --------
                         /
                        /
                       / Tunnel=2, callid=5
                  -------------
                 |  New        |
                 |Serving LAC2 |
                  -------------
```

```
Client     S-LAC2          A-LAC         LAC1       LNS
   Link Layer
      Msg1       SCCRQ
   --------->  ---------->
                SCCRP (Mobile AVP)
               <---------
                SCCCN
               ------------>
                ICRQ (with User AVP)
               ------------->     CDN
                              ------------>
                ICRP
              <-------------
                ICCN             Auth_Req (Optional)
               ------------->  ------------------------->
                 ACK
                <----------
  Link Layer
    Msg2
 <---------
```

2-hop to 2-hop Handover Scenario
Fig 4 Independent Tunnel Approach

In Fig 4, we show a 2-hop to 2-hop handover scenario. When the Anchor LAC receives the ICRQ with an attached User AVP, and finds an entry in the mapping table, it concludes that this is a 2-hop to 2-hop handover scenario. Therefore, the Anchor LAC sends a CDN message to the old LAC, and updates the mapping table with the new tunnel and call identities carried within the ICRQ message. Again, if a user-level re-authentication is desired, the Anchor LAC can send an Authentication Request message to the LNS to trigger such a reaction.

The advantages of ITA are:
(a) the handover latency is reduced due to a shorter hop distance between the Serving LAC and the Anchor LAC. The hop between the Anchor LAC and the LNS remains unchanged.
(b) Roaming service can be more flexible. As long as there is an agreement between the home WSP and the corporate network, and between the home WSP and other WSPs, the subscribers can roam to more places without having to terminate the PPP session.

The disadvantages of ITA are
(a) more complex than the Simple AVP approach
(b) the Anchor LAC needs to maintain 2N flow-controlled data sessions for N PPP calls.

2.3 Concatenated Tunnel Approach (CTA)
In the Concatenated Tunnel Approach, there is only one L2TP session per call but this L2TP session spans two hops: one between the Serving LAC and the Anchor LAC; one between the Anchor LAC and LNS. This approach requires more software enhancements to the Anchor LAC. However, the advantage is that it has end-to-end flow control and less CPU processing than the ITA.

```
 ----------          --------
| Anchor  | Tunnel=1  | LNS   |
| LAC     |-----------|       |
 ---------  callid=3   --------
     |
     |
     |  Tunnel=3, callid=1
  -------------
 |Serving LAC |
  -------------
```

```
Client     S-LAC           A-LAC         LNS
   Link Layer
      Msg1       SCCRQ
   --------->   ---------->
                 SCCRP (with Mobile AVP)
                <---------
                 SCCCN
                ------------>
                 ICRQ (with User AVP)
                ------------->
                 ICRP (with Seq No, ACCM, Proxy Auth AVPs)
               <-------------
                 ICCN           Auth_Req (Optional)
                -------------->  -------->
                   ACK
                 <-----------
  Link Layer
    Msg2
 <----------
```

One hop to 2-hop Handover Scenario
Fig 5 Independent Tunnel Approach

The main differences between CTA and ITA are:
(i) For CTA, there is only one flow control procedure for the 2 hop. Thus, he Anchor LAC needs to send a Sequence Number AVP (which contains information on the latest Nr,Ns used before the handover) to the Serving LAC so that the Serving LAC knows what sequence numbers to start with.
(ii) For CTA, the Anchor LAC merely observes and updates the latest (Nr, Ns) information within the data packets traversing in either direction. It does not have to perform flow control actions on two data sessions as in the ITA.

The advantages of CTA are:
(a) we have an end/end flow control for the PPP call
(b) the handover latency is reduced because of a shorter path between the Serving LAC and the Anchor LAC.
(c) Roaming service can be more flexible. As long as there is an agreement between the home WSP and the corporate network, and between the home WSP and other WSPs, the subscribers can roam to more places without service interruptions.
(d) it requires less CPU processing than ITA.

The disadvantages of CTA are:
(a) more complex than the Simple AVP and ITA approaches.

3 Service Model Issues

3.1 Authentication

As in [1], the authentication of the user occurs in four phases; the first at the visiting WSP, the second at the Home WSP, and the third and optionally the fourth at the LNS.

3.2 Accounting

It is a requirement that the Serving LAC, the Anchor LAC and the LNS be capable of providing accounting data and hence all three parties may count packets, octets and connection start and stop times.

Accounting statistics collected by the Serving LAC and the Anchor LAC are sent to their AAA Servers. The accounting Server in the Foreign Network may forward accounting statistics to the Home Accounting Server periodically (weekly, monthly).

4.0 Control Message Processing

For the 3-hop scenario, we assume that any party, namely the Serving LAC, the Anchor LAC or the LNS can terminate the session by sending a Call Disconnect Notify. If the Anchor LAC desires to terminate the session, then the Anchor LAC has to send a Call Disconnect Notify message to both the Serving LAC and the LNS.

Note that in the three hop scenario, the Hello messages for the control connections between the Serving/Anchor LACs and between the Anchor LAC and LNS are done independently of one another for both the Independent and Concatenated Tunnel approaches. The Anchor LAC is expected to relay all the Set-Link-Info, and Wan-Error-Notify messages.

4.1 Newly Defined Control Message and AVPs.

To support the tunnel extension and call transfer features, we define one optional control message, namely the Auth_Request message. This message allows the LAC to inform the LNS to trigger a PPP level re-authentication with the PPP client during handover.

In addition, we define four new AVPs: (i) Mobile AVP, (ii) User AVP, (iii) Sequence Number AVP, (iv) A-LAC Window AVP. The Sequence No, A-LAC Window are used only in the CTA. We refer the readers to Appendix 1 for more information on when these 3 AVPs are used in the CTA.

4.1.1 Authentication Request (Auth_REQ)

Authentication Request message is sent from a LAC to an LNS to trigger the LNS from initiating a PPP reauthentication with an existing user.

```
Message Format for Authentication Request
++++++++++++++++++++++++++++++++++++++
|L2TP control message header         |
++++++++++++++++++++++++++++++++++++++
|Authentication  Request             |
++++++++++++++++++++++++++++++++++++++
```

4.1.2 Newly Defined AVPs

The new AVP is encoded as Vendor ID 1751 which reflects Lucent Systems, the initial developer of this specification, and it should be changed to 0 and an official Attribute value chosen if this specification advances on a standards track).

```
 0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |M|H|0|0|0|0|  Overall Length   |           Vendor ID           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |           Attribute           | Value...                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | [until Overall Length is reached]...                          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The first six bits are a bit mask, describing the general attributes of the AVP.

The three newly defined AVPs are:

Attr	M	Len	Attribute Name
40	1	8	Mobile AVP
41	1	16+	User AVP
42	1	10	Sequence Number AVP
43	1	8	Receive Window Size AVP allowed by the Anchor LAC

The existing Receive Window Size AVP in [1] with Atribute vallue 10 is used to communicate the receive window size allowed by the LNS.

4.1.2.1 Mobile AVP

This AVP is used by the LNS/A-LAC to inform a LAC that the LNS/A-LAC supports the mobility feature.

Message Format for Mobile AVP

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |1|1|0|0|         Length        |          Lucent-Vendor ID     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                 40            |          Support Mobility     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.1.2.2 User's AVP

This AVP is used to provide user's name and user's credentials. The user's credentials may include information like user's identity (IMSI), phone number. This AVP may be a hidden AVP (according to Section 5.7 in the L2TP draft [1]).

Message Format for User's AVP

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |1|1|0|0|         Length        |          Lucent-Vendor ID     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                 41            |          User-Service          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                  ASCII Representation of 15 digit No          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                  Phone          Number                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

User's AVP

- contains information about the user's name and user's credentials e.g. multihop virtual dial up service, user's identity (MIN), service provider's phone number, user level authentication information, etc

4.1.2.3 Sequence Number AVP

This AVP is used to convey (Nr, Ns) information to the new Serving LAC. This AVP is only used in the Concatenated Tunnel approach and is attached to the ICRP message.

Message Format for Sequence Number AVP

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |1|1|0|0|         Length        |        Lucent-Vendor ID       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |               42              |             Reserved          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             Nr                |                   Ns          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Nr - next received sequence number to be expected.
Ns - next sending sequence number.

4.1.2.3 A-LAC Window's AVP

This AVP is used by the Anchor LAC to inform the new Serving LAC of the A-LAC's payload window size. The original Receive Window AVP is used to convey LNS's window size. The format is exactly the same as the Receive Window AVP stated in [1]. This AVP is only required for the Concatenated Tunnel approach and is attached to the ICRP message.

5. Security Issues

In our proposal, the Serving and Anchor LACs may belong to the same WSP or they may belong to different WSPs. For the case where they belong to the same WSP, we do not introduce any new security threats. For the case where they belong to different WSPs, we assume that if a corporate net trusts a particular WSP,say WSP1, and WSP1 trusts another WSP, WSP2, then the corporate network trusts WSP2. IP security can be supported between Serving LAC and LNS for the triplet case using extended ideas described in the draft "Securing L2TP using IPSEC" [2].

6. Acknowledgements

The author wishes to thank George Gross, Jim Kallimani and Margaret Yang for very useful comments.

7. Contacts

M. C. Chuah
Lucent Technologies
101, Crawfords Corner Road,
Holmdel, NJ 07733
chuah@lucent.com
(732)-949-7206

Don Grosser
IBM Corporation
3039 Cornwallis Road,
Research Triangle Park, NC 27709
grosser@us.ibm.com
(919)-254-2160

G. Rai
1101 Warrenville Road,
Naperville, IL

grai@lucent.com
(630)-979-8131

Jacob Teplitsky
RABU
Lucent Technologies
4464 Willow Rd,
Pleasanton, CA 94588
jacobt@livingston.com
(925) 737-2189

8. References

[1] A. Valencia, etal, Layer Two Tunneling Protocol, Internet draft, draft-ietf-pppext-l2tp-12.txt, October, 1998
[2] B. Patel, B. Aboba Security L2TP using IPSEC, Internet draft, draft-ietf-pppext-l2tp-security-01.txt, March 1998

Appendix 1 Using CTA in a Handover Scenario

Assume that the subscriber has a PPP call which spans two hops between the S-LAC1, A-LAC and the LNS. Then, the subscriber moves to the coverage area of a new LAC, S-LAC2.

Message Flows for this handover scenario:

```
    S-LAC2           A-LAC        S-LAC1        LNS
 Link Msg1    ICRQ
-->          Orig ICRQ
             User's AVP
            --------->
                           CDN
                         --------->

 Link Msg2    ICRP
<-            Orig ICRP
              Seq No AVP
              A-LAC Window AVP
              LNS Window AVP
              ACCM AVP
             <----------

 Link Msg3      ICCN
-->          Orig ICCN        Auth_Req (optional)
             ---------->  ------------------------->

              ACK
             <----------
```

Orig ICRQ - means the ICRQ message as stated in [1]
Orig ICRP - means the ICRP message as stated in [1]
Orig ICCN - means the ICRP message as stated in [1]

Appendix 2 Transfer of Sequence Number During Handover

Here, we describe how the sequence numbers are updated during a handover if CTA is used.

A2.1 Handover from a 2-hop to a 3-hop configuration.

Old LAC	LNS
Ss=13	Ss=7
Sr=6	Sr=10

The old LAC (which is now the A-LAC) will set Nr=6, Ns=13 in the Sequence Number AVP within the ICRP message. After the handover,

New S-LAC	A-LAC(Old LAC)		LNS
Ss=13	Ss^S=13	Ss^L=7+	Ss=7+
Sr=6	Sr^S=6	Sr^L=10+	Sr=10+

A2.2 Handover from a 3-hop to a 2-hop configuration.

Old S-LAC	A-LAC		LNS
Ss=13	Ss^S=12	Ss^L=6	Ss=7
Sr=5	Sr^S=4	Sr^L=9	Sr=10

The Anchor LAC will set (Ss=Ss^S, Sr=Ss^L) and drop the 4 tuple (Ss^L, Sr^L,Ss^S,Sr^S) as shown below:

A-LAC(LAC)	LNS
Ss=12	Ss=7+
Sr=6	Sr=10+

A2.3 Handover from a 3-hop to another 3-hop configuration.

New S-LAC	Old S-LAC	A-LAC		LNS
	Ss=13	Ss^S=12	Ss^L=6	Ss=7
	Sr=5	Sr^S=4	Sr^L=9	Sr=10

The A-LAC sets Ns=Ss^S=12, Nr= Ss^L=6 in the Sequence Number AVP within the ICRP message which is sent to the new S-LAC. After the handover, we have

New S-LAC	A-LAC		LNS
Ss=12	Ss^S=12	Ss^L=6+	Ss=7+
Sr=6	Sr^S=6	Sr^L=9+	Sr=10+

Appendix 3 Multiple LNS Scenario

For the case where a LAC may potentially communicate with more than one LNSs, the mobile feature will still work as long as the order at which any LAC tries a possible list of LNSs is the same.